**CONTINUATION OF APPLICATION FOR A SEARCH WARRANT**

1. I, Brent Erk, a Task Force Officer (TFO) with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), being duly sworn, depose and state as follows:
2. I have been an ATF TFO since 2018. My duties include the investigation of various violations of federal criminal law, including matters involving violations of 18 U.S.C. § 922(g)(1), which makes it illegal for a person who has been convicted of a crime punishable by more than a year of incarceration to possess a firearm, hereinafter, the "Subject Offense."
3. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of the following electronic devices and their contents:
    a. a white, Apple iPhone with serial number 353237205410857 (**SUBJECT DEVICE 1)**.
    b. a black Samsung phone with a cracked screen and unidentifiable serial number (**SUBJECT DEVICE 2)**.
4. The information contained in this continuation is based upon information obtained personally by me and information provided to me by other law enforcement officers and agents who have participated in this investigation. This continuation does not contain all the information known as a result of this investigation, but only those facts that I believe are necessary to establish probable cause for the search warrant sought.
5. Based on my training and experience, I know that individuals who possess firearms often maintain possession of them for extended periods of time. I

know that individuals who possess firearms may also possess other items associated with their firearms, including ammunition, magazines, holsters, cases, and records indicating purchase, use, maintenance, or sale of such items. Such records of purchase, maintenance, sale, etc. may be retained electronically. I also know that individuals who illegally possess firearms frequently possess photographs, films, or videos of themselves in possession of the firearms or using the firearms, which they frequently store on their smartphones. I also know that individuals who illegally possess firearms often communicate with others using their smartphones (using, for example, phone calls, text messages, voicemail messages, electric mail, and phone applications) about firearms.

**BACKGROUND OF INVESTIGATION**

6. This investigation relates to alleged violations of the federal firearms laws by Terrell D. MCQUEEN, date of birth XX/XX/1991,[1] of Lansing, Michigan. MCQUEEN has multiple prior felony convictions, including: felony controlled substance possession (cocaine, heroin or other narcotic less than 25 grams) in 2008 in the 30th Circuit Court, Ingham County, Michigan; and felony armed robbery in 2010 in the 30th Circuit Court, Ingham County, Michigan.

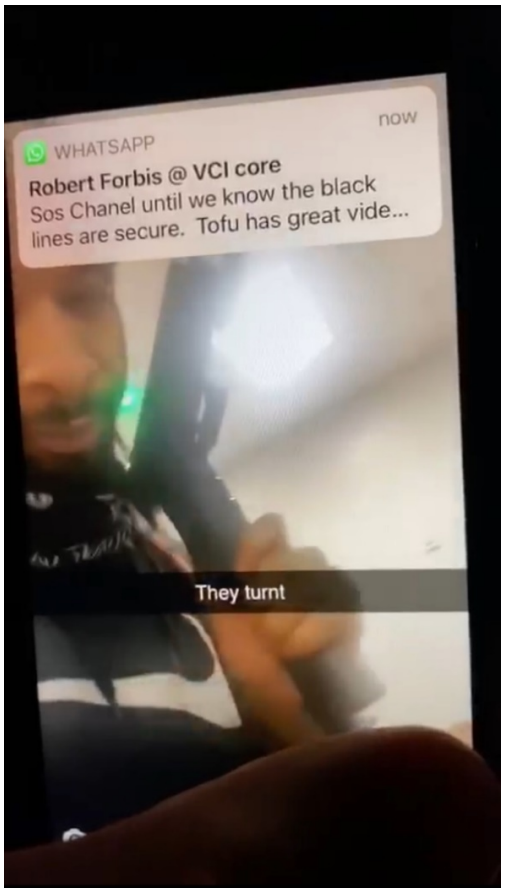
7. On or about December 22, 2020, the Lansing Police Department (Lansing PD) Violent Crime Impact Team and the Michigan State Police (MSP) Secure Cities

[1] MCQUEEN's full date of birth is known to me but is not included here to protect his personally identifiable information.

Partnership received information from a sergeant on the Violent Crime Team that the Snapchat account for Terrell MCQUEEN, with username "toedoe," posted a video involving a firearm. Prior to seeing that Snapchat video, the sergeant had been monitoring the account with username "toedoe" and observed other videos depicting MCQUEEN with various firearms. Lansing PD Violent Crime Team officers were familiar with MCQUEEN'S appearance based on prior law enforcement interactions.

8. I obtained a copy of the December 22, 2020 Snapchat video. The video depicts MCQUEEN inside a building with several other unidentified subjects holding long guns and pistols. I have confirmed MCQUEEN is the individual in the video based on evidence photographs and video taken in connection with his subsequent arrest later that same day. The video clearly shows MCQUEEN holding a pistol containing an extended magazine. In the video, MCQUEEN is wearing a dark Nike sweatshirt with a swoosh across the front. The Snapchat video was titled "They turnt."

9. The following page contains screenshots from the Snapchat video:





10. Because Snapchat is a social media/messaging application available in app stores for mobile devices (see paragraphs 14-16 below), there is probable cause to believe that additional evidence from Snapchat (or original recordings of videos before they were edited into "Snaps") could be found on mobile devices possessed by MCQUEEN.

11. On December 22, 2020, at approximately 11:00 PM, Lansing PD/MSP Violent Crime Impact Team officers began searching for Terrell MCQUEEN to arrest him on an active outstanding arrest warrant issued in Ingham County, Michigan.

a. Lansing PD/MSP Violent Crime Impact Team officers observed MCQUEEN driving a dark grey 2020 Jeep Compass with license plate number EFQ2965. Lansing PD/MSP officers further observed MCQUEEN pull into the parking lot of the Admiral gas station located at 3400 S. Waverly Rd. in Lansing, Michigan. They then observed MCQUEEN enter the gas station.

b. Lansing PD/MSP officers made contact with MCQUEEN inside the gas station. MCQUEEN initially resisted arrest but was subsequently taken into custody and arrested on his outstanding warrant.

c. Upon searching MCQUEEN's person incident to arrest, Lansing PD/MSP officers located a firearm inside his front sweatshirt pocket. The firearm is specifically described as a Glock Model 22, semi-automatic pistol with serial number XUG901 containing an extended magazine loaded with twenty-one .40 caliber live rounds of ammunition.

d. MCQUEEN was wearing the same Nike sweatshirt with a swoosh across the front as he was wearing in his Snapchat video titled "They turnt" from earlier that day. Lansing PD took the following photograph after MCQUEEN's arrest, which shows him wearing the same sweatshirt:

12. I consulted with ATF Special Agent Heidi Wallace, who is a certified firearms NEXUS expert. She determined the firearm recovered from MCQUEEN's person was distributed from the State of Georgia and therefore traveled in interstate commerce prior to MCQUEEN's possession of it.

13. Lansing PD/MSP officers searched the 2020 Jeep Compass that MCQUEEN drove to the gas station where he was arrested; Khouri Paschall was in the front passenger seat of the Jeep. Lansing PD/MSP officers located an additional Glock semi-automatic pistol on the passenger side of the vehicle, illegal narcotics, a magazine of ammunition, and two cellular telephones (**SUBJECT DEVICE 1** and **SUBJECT DEVICE 2**) that Terrell MCQUEEN identified as his phones. The two cellular phones are currently in the custody of the Lansing Police Department.

**BACKGROUND ON MESSAGING APPLICATIONS GENERALLY AND SNAPCHAT SPECFICALLY**

14. Instagram, Twitter, Facebook, Snapchat, and text messaging are common tools used by mobile devices with access to the internet, such as smart phones or tablets. Users of Instagram, Twitter, Snapchat, and Facebook must register a password protected account which they can access with a smartphone data plan or Wi-Fi Internet access to send and receive messages, photographs, videos, sketches, mobile webpages, and other content. Oftentimes, with a smartphone that has a data plan with a wireless provider, users of these social media platforms can use text messages services included in their phone plan to send and receive messages, photographs, videos, sketches, mobile webpages, and other content, just as happens through social media accounts.

15. The social media accounts are often used as a platform to maintain an online social media profile which can be viewed by "friends" or "followers" and they can use their online profile to share photographs and videos or engage in chat sessions, meet other people, among other things. While posting status updates, comments, or likes on their profile, social media users can allow others to view their profiles or keep them private. Since social media accounts can contain location data and are commonly viewed by peers, more personal communication can occur with direct messaging through the social media application, or through text messages.

16. The Snapchat Law Enforcement Guide, published by Snapchat, Inc., states that "Snapchat is a mobile application made by Snap Inc. ("Snap") and

available through the iPhone App Store and Google Play Store. The Snapchat app provides users a way to share moments with photos, videos, and chats."

**ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

17. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

18. There is probable cause to believe that things that were once stored on the Subject Devices may still be stored there, for at least the following reasons:

    a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

    b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before

they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or "cache."

19. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how a Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Subject Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a

deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

20. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

## CONCLUSION

21. Based upon the above information, I respectfully submit that there is probable cause to search **SUBJECT DEVICE 1** and **SUBJECT DEVICE 2** described in Attachment A for the evidence and user attribution items identified in Attachment B.